IMPLEMENTASI METODE FORENSIK JARINGAN UNTUK MEMONITORING KOMPUTER WINDOWS SERVER

Brian Abimayu Mahendra*[1]; Harso Kurniadi[2]; Yudo Bismo Utomo[3]
[1,2,3]Program Studi Teknik Komputer, Fakultas Teknik, Universitas Islam Kadiri-Kediri Jawa Timur
Email: brianutred@gmail.com, yudobismo@uniska-kediri.ac.id, harsokurniadi@uniska-kediri.ac.id

ABSTRACT

The use of global computer networks, such as the internet, makes it easier to complete various jobs. However, this convenience also triggers misuse of unauthorized access to commit certain crimes. To prevent this, network administrators need to implement strategies to ensure the network remains safe from unauthorized access. One commonly used network security system is a firewall, which functions to protect data from users who do not have access rights. One type of attack that often occurs is a Denial of Service (DoS) attack which aims to drain computer resources by targeting the Windows server in an agency, so that other users have difficulty accessing the computer being attacked. In maintaining the integrity, confidentiality and availability of data, monitoring network security is a crucial aspect. This research proposes the use of network forensic methods for network traffic analysis in detecting and responding to security incidents. This research uses Wireshark, a network traffic analysis tool, to detect Distributed Denial of Service (DDoS) attacks. Wireshark is able to capture and examine data packets passing through the network, so it can identify DDoS attack patterns such as abnormal traffic spikes and suspicious packets. Through DDoS attack simulations, this research shows how network forensic methods can be used effectively to detect, analyze and respond to cyber attacks.

Keywords: *Network Security, Firewall, Denial of Service, Network Forensics.*

ABSTRAK

Penggunaan jaringan komputer secara global, seperti internet, memberikan kemudahan dalam menyelesaikan berbagai pekerjaan. Namun, kemudahan ini juga memicu adanya penyalahgunaan akses tidak sah (un-authorized access) untuk melakukan kejahatan tertentu. Untuk mencegah hal tersebut, administrator jaringan perlu menerapkan strategi guna memastikan jaringan tetap aman dari akses yang tidak berwenang. Salah satu sistem pengamanan jaringan yang umum digunakan adalah firewall, yang berfungsi melindungi data dari pengguna yang tidak memiliki hak akses. Salah satu jenis serangan yang sering terjadi seperti serangan Denial of Service (DoS) yang bertujuan menguras sumber daya komputer dengan menargetkan pada windows server di suatu instansi, sehingga pengguna lain kesulitan mengakses komputer yang diserang. Dalam menjaga integritas, kerahasiaan, dan ketersediaan data, monitoring keamanan jaringan menjadi aspek krusial. Penelitian ini mengusulkan penggunaan metode forensik jaringan untuk analisis lalu lintas jaringan dalam mendeteksi dan merespons insiden keamanan. Penelitian ini menggunakan Wireshark, sebuah alat analisis lalu lintas jaringan, untuk mendeteksi serangan Distributed Denial of Service (DDoS). Wireshark mampu menangkap dan memeriksa paket data yang melintas di jaringan, sehingga dapat mengidentifikasi pola serangan DDoS seperti lonjakan lalu lintas yang tidak normal dan paket mencurigakan. Melalui simulasi serangan DDoS, penelitian ini menunjukkan bagaimana metode forensik jaringan dapat digunakan secara efektif untuk mendeteksi, menganalisis, dan merespons serangan siber.

Kata Kunci: *Network Security, Firewall, Denial of Service, Forensik Jaringan.*

1. PENDAHULUAN

Internet membawa dampak positif dengan mempermudah penyelesaian berbagai pekerjaan. Namun, kemudahan ini juga membuka peluang bagi sebagian pihak untuk menyalahgunakan akses demi tujuan kejahatan tertentu. Untuk mencegah hal tersebut, seorang administrator jaringan perlu menerapkan strategi dan keterampilan untuk memastikan keamanan jaringan, sehingga tidak mudah ditembus oleh pihak yang tidak berhak. Saat ini, jaringan komputer berkembang pesat dan digunakan secara luas, baik di lembaga komersial, dunia pendidikan, maupun di rumah-rumah yang membutuhkan akses internet.

Internet dapat diakses oleh berbagai kalangan, termasuk hacker dan cracker. Dengan berbagai motivasi, mereka kerap melakukan penyusupan yang berpotensi merugikan pemilik server dan jaringan komputer. Serangan ini dilakukan menggunakan beragam metode, baik melalui alat yang mereka kembangkan sendiri maupun perangkat lunak yang tersedia di pasaran.[1][2][3]

Firewall adalah metode untuk menerapkan kebijakan keamanan jaringan yang disesuaikan dengan fasilitas yang tersedia, serta mempertimbangkan dampak yang ditimbulkan oleh kebijakan tersebut. Semakin baik dan terukur kebijakan keamanan yang diterapkan, semakin terbatas pula layanan konfigurasi jaringan yang dapat diakses, karena adanya pembatasan yang diberlakukan. Firewall berfungsi sebagai penyaring antara komputer internal dan eksternal. Selain itu, firewall juga berperan dalam mengatur dan mengontrol lalu lintas data yang diizinkan untuk mengakses jaringan privat. Proses kontrol dilakukan berdasarkan alamat IP sumber, port TCP/UDP dari sumber dan tujuan, serta informasi header yang terdapat dalam paket data. Sebagai penyaring, firewall bermanfaat untuk mencegah lalu lintas yang masuk ke subnet jaringan tertentu, sehingga dapat melindungi file-file rahasia dari akses yang tidak diinginkan.[4][5][6]

Salah satu bentuk serangan yang dapat terjadi dalam sebuah jaringan adalah serangan DoS (Denial of Service). Serangan ini bertujuan menghabiskan sumber daya (resource) komputer hingga menyebabkan malfungsi melalui jaringan internet. Serangan DDoS (Distributed Denial of Service) merupakan salah satu ancaman paling serius terhadap keamanan jaringan, dengan jumlah korban yang terus meningkat setiap harinya. Deteksi anomali dari sekumpulan data menjadi isu yang sangat krusial dalam setiap pendekatan solusi keamanan jaringan.

Semua teknik mitigasi membutuhkan tindakan tertentu, seperti blackholing untuk penyedia upstream atau pemberitahuan perubahan rute. Jika tindakan ini dilakukan secara manual oleh manusia, prosesnya cenderung memakan waktu lama. Serangan DDoS yang menargetkan router sering kali diatasi dengan menggunakan firewall pada MikroTik. Dalam jaringan yang melibatkan keamanan lapisan 3 dan lapisan 4, penerapan rate shaping dapat membantu mencegah serangan berbasis banjir TCP. Selain itu, pembatasan koneksi dapat menjadi metode mitigasi yang efektif. Namun, manipulasi ukuran data yang diarahkan ke target serangan DDoS dapat memperburuk tingkat serangan, menyebabkan router yang dilewati data tersebut mengalami peningkatan konsumsi daya listrik dan beban pada komputer.[7][8][9]

Dan dalam peneltian ini terfokuskan pada cara Implementasi metode forensik jaringan untuk memonitoring komputer windows server. Metode forensik jaringan adalah proses menangkap, mencatat, dan menganalisis aktivitas dalam jaringan untuk mengidentifikasi sumber serangan keamanan atau menyelidiki masalah lain yang terjadi[10][11]. Dimana penelitian ini menganalisis tentang banyaknya masalah yang terjadi salah satunya serangan DDoS yang mentargetkan windows server.

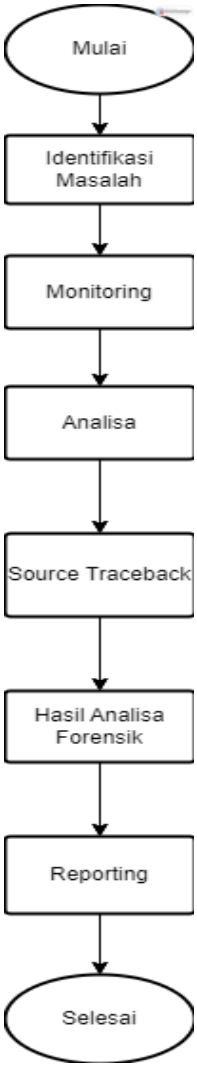
Penyerang dalam serangan DDoS sering kali menargetkan Windows Server karena server tersebut menyimpan banyak data penting berupa bukti digital. Oleh karena itu, dengan memanfaatkan alat seperti Wireshark, peneliti dapat melakukan pemantauan dan analisis forensik jaringan untuk mendeteksi anomali lalu lintas. Sejak tahun 1980-an hingga 1990-an, metode serangan telah berkembang, mencakup teknik seperti peretasan kata sandi, pengungkapan kata sandi, eksploitasi kerentanan, menonaktifkan audit, pencurian data, hingga pembajakan sesi pengguna.

Kebaruan dari penelitian ini yaitu dimana kita bisa mencegah serangan DDoS dengan menggunakan tools yang dinamakan wireshark dengan memonitoring nomor ip yang masuk,

agar mudah untuk melakukan investigasi ataupun merekam lalu lintas jaringan (traffic).

2. METODE PENELITIAN

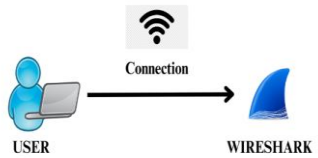
Penelitian ini menggunakan metode Waterfall dalam Network Development Life Cycle (NDLC). Waterfall adalah salah satu metode yang diterapkan dalam pengembangan perangkat lunak, yang juga dikenal sebagai siklus pengembangan jaringan. Model ini dinamakan Waterfall karena proses pengembangannya mengikuti alur seperti air terjun, di mana setiap tahap dilakukan secara berurutan dari tahap awal hingga tahap akhir.



Gambar 1 Alur Penelitian

2.1 Monitoring

Monitoring jaringan biasanya digunakan untuk menjaga keamanan jaringan, terutama oleh pengguna komputer yang mengalami serangan. Proses ini berfungsi sebagai langkah perlindungan terhadap jaringan. Salah satu perangkat lunak yang dapat digunakan untuk monitoring adalah Wireshark, yang memerlukan koneksi ke jaringan internet agar dapat dioperasikan. Jika jaringan menunjukkan kinerja yang buruk atau sering mengalami masalah, pendekatan yang lebih baik adalah berfokus pada optimalisasi kinerja dan operasional jaringan, bukan sekadar menyelesaikan masalah yang ada. Dengan kata lain, diperlukan pendekatan holistik dalam menangani masalah jaringan. Alih-alih hanya mengisolasi masalah tertentu, lebih efektif untuk memeriksa seluruh jaringan menggunakan alat seperti protocol analyzer atau perangkat pemantauan. Hal ini bertujuan untuk meningkatkan kinerja jaringan. Namun, lambatnya koneksi internet sering kali disebabkan oleh sebagian pengguna yang mengambil data secara berlebihan, sehingga kapasitas jaringan tidak seimbang dengan jumlah penggunanya.



Gambar 2 Alur Monitoring

2.2 Analisa

Proses analisis bukti digital ini melibatkan pengumpulan data lalu lintas jaringan menggunakan Wireshark setelah setiap skenario serangan selesai. Data yang diperoleh kemudian dianalisis menggunakan pendekatan anomaly-based detection untuk mengidentifikasi pola yang menyimpang dari kondisi normal server. Analisis forensik dilakukan dengan menganalisis paket data yang ditangkap oleh Wireshark, sedangkan analisis kinerja server dilakukan dengan mengamati penggunaan sumber daya sistem seperti yang ditampilkan oleh Task Manager atau alat monitoring kinerja lainnya.

2.3 Source Traceback

Proses analisis data forensik jaringan bertujuan untuk mengungkap kronologi dan

mekanisme serangan siber. Hasil analisis ini akan menjadi dasar bagi tim keamanan untuk melakukan tindakan remediasi dan mitigasi. Salah satu teknik yang sering digunakan untuk mengidentifikasi sumber serangan adalah traceback. Dengan traceback, kita dapat melacak jalur serangan dari target hingga ke sumbernya, sehingga memungkinkan kita untuk mengambil tindakan pencegahan yang lebih efektif.

2.4 Hasil Analisa Forensik

Hasil Analisa forensik mencangkup tiga tahapan penting dalam investigasi yaitu collection, preservation, dan examination. Pada tahap collection, bukti elektronik dan data relavan dikumpulkan dari berbagai sumber seperti jaringan komputer atau komunikasi digital. Pengumpulan ini bertujuan untuk mendukung investigasi forensik jaringan dengan menyediakan informasi yang akurat dan lengkap. Aplikasi wireshark melibatkan pengguna wireshark sebagai alat analisis paket jaringan untuk menyelidiki, memantau, dan mendeteksi insiden keamanan. Pengumpulan penting untuk mendeteksi kegiatan yang mencurigakan, serangan keamanan, atau pelanggalaran kebijakan.

Setelah bukti terkumpul, proses berlanjut ke tahap preservation, di mana barang bukti, baik yang berupa fisik maupun digital, dijaga keamanannya. Tahap ini sangat penting untuk memastikan bahwa bukti digital tidak rusak atau berubah, sehingga validitas dan integritasnya tetap terjaga sepanjang proses investigasi. Keamanan bukti digital selama tahap ini memastikan bahwa informasi yang diperoleh relavan, terutama ketika melibatkan bukti digital atau data jaringan.

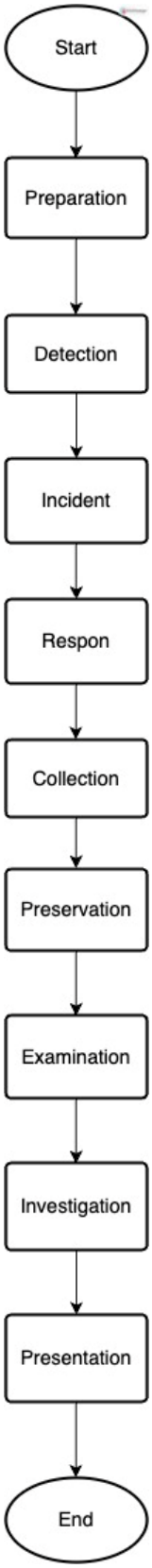
Tahap terakhir adalah examination, yang melibatkan pengujian mendalam terhadap keabsahan dan keutuhan data yang telah dikumpulkan. Selain itu, keterkaitan data dengan tindak kriminal yang sedang diselidiki juga dianalisis. Melalui proses ini, penyidik dapat memastikan bahwa bukti yang diperoleh memiliki relevansi yang kuat dengan kasus yang sedang ditangani, sehingga dapat digunakan secara efektif dalam proses penegakan hukum. Dalam kegiatan ini untuk merekam dan menyimpan bukti digital dari suatu tindakan kejadian atau insiden kejadian tertentu dalam jaringan. Ketiga tahapan ini bekerja sama untuk memberikan fondasi yang kuat bagi keberhasilan investigasi forensik.

2.5 Reporting

Reporting adalah tahapan terakhir dari Forensik Jaringan, dalam tahapan ini kita akan mereprentasikan informasi yang merupakan hasil dari proses analisis.

Berdasarkan kebutuhan diatas, maka suatu system forensik jaringan setidaknya terdapat beberapa proses, yaitu:

1. Preparation: tahap ini dilakukan sebagai persiapan dan pengecekan alat software dan hardware yang akan digunakan.
2. Detection: Proses mengidentifikasi, menganalsis, dan merespon insiden keamanan atau kejadian mencurigakan dalam jaringan komputer
3. Incident: proses menyelidiki dan menganalisis kejadian yang mencurigakan atau serangan yang terjadi dalam jaringan komputer atau system komunikasi digital.
4. Respon: Langkah yang diambil setelah terjadinya insiden keamanan atau aktifitas yang mencurigakan dalam jaringan komputer.
5. Collection: Proses pengumpulan bukti electronic dan data yang relavan dari jaringan komputer atau system komunikasi digital untuk mendukung investigasi.
6. Preservation: tahap ini, barang bukti baik yang berupa fisik maupun digital akan dijaga keamanan, dan keutuhannya pada setiap tahapan proses investigasi, sehingga validitas dan integritas barang bukti tetap terjaga.
7. Examination: tahap ini adalah tahap pengujian pengujian keabsahan data, keutuhan data keterkaitan data dengan tindak kriminal suatu kasus.
8. Investigation: proses menyelidiki dan menganalisis bukti digital yang ditemukan dalam jaringan computer atau system komunikasi digital untuk memahami insiden keamanan atau aktivitas yang mencurigakan.
9. Presentation: tahap presentasi bukti digital kepada pihak yang berwenang dengan menggunakan Bahasa yang dapat dipahami.



Gambar 3 Alur Diagram Forensik Jaringan

3. HASIL DAN PEMBAHASAN

Pada tahap ini, Peneliti menggunakan Sembilan tahapan yang sesuai dengan metode forensik jaringan yaitu Preparation, Detection, Incident, Respon, Collection, Preservation, Examination, Investigation, Presentation.

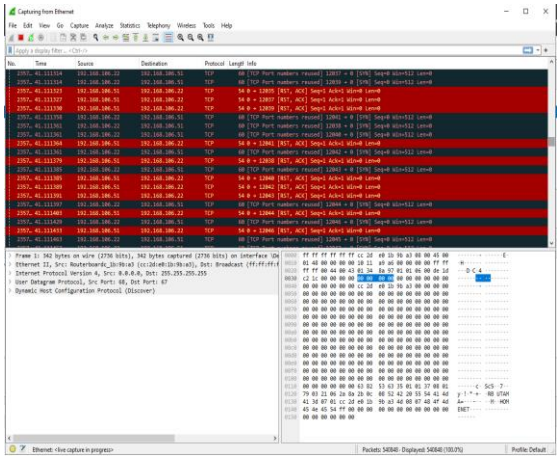
3.1 Preparation

Alat yang digunakan peneliti terdiri dari beberapa perangkat keras (Hardware), Perangkat Lunak (Software), dan Tools sebagai berikut:

a. Perangkat keras (Hardware)
   Pada penelitian ini, peneliti menggunakan perangkat keras terdiri dari sebuah PC1 dengan processor Core i5, Ram 8gb, Hardisk 1 TB sebagai windows server dan PC2 dengan prosesor Core i5, Ram 8gb, Harddisk 1TB sebagai penyerang
b. Perangkat Lunak (Software)
   Perangkat lunak yang digunakan pada penelitian ini terdiri dari wireshark version 4.2.5 dan operation sistem kali linux 2024.
c. Tools
   Penelitian ini menggunakan beberapa tools yang digunakan yaitu CMD (Command Promt) pada system operasi dan tools hping3 pada kali.

3.2 Detection

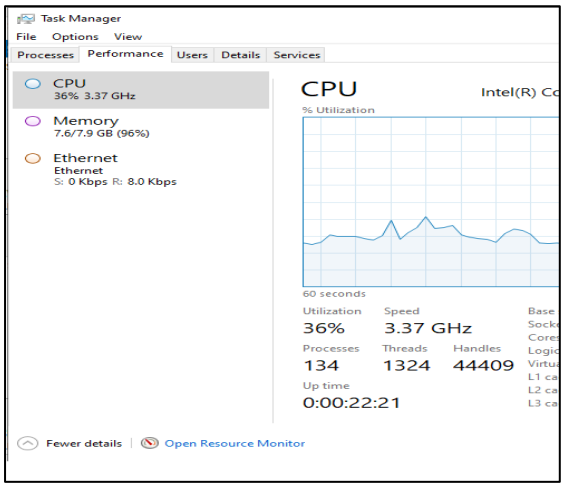
Pada tahap ini, peneliti memonitoring jaringan dan mendeteksi adanya peningkatan trafik yang tidak biasa atau anomaly traffic, serta terjadi penurunan kinerja hardware atau perangkat. Peneliti menggunakan perangkat lunak wireshark untuk mendeteksi adanya trafik terkirim dan diterima terlalu tinggi dan serangan tersebut merupakan serangan DoS (Ping of Death) yang di Analisa pada tahap investigation. Berikut tampilan bukti kenaikan traffic yang terlalu tinggi diambil dari log wireshark terlihat bahwa setiap 1 detik terjadi 3 paket yang terkirim dan diterima, yang terkirim dan diterima dengan rentang waktu 1 menit sekitar 180 kali paket terkirim dan diterima. Hal tersebut tidaklah normal dalam pengiriman dan penerimaan paket ke server.



Gambar 4. Tahap Detection

3.3 Incident

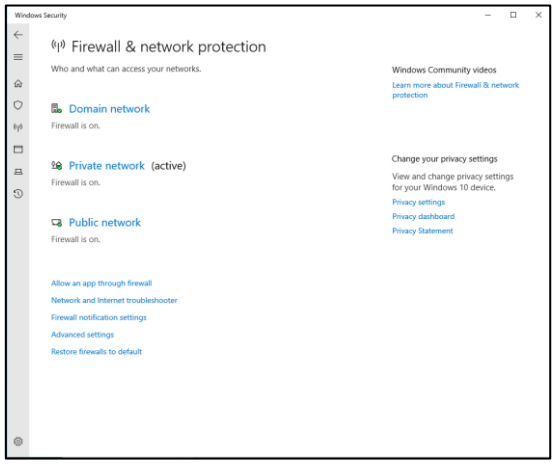
Peneliti menganalisa dan menyelediki komputer server yang terkena serangan ddos mengalami kelemotan pada system. Tidak hanya itu terdapat juga peningkatan CPU dan Memory. Berikut evidence atau bukti penggunaan CPU yang terlalu tinggi sehingga mencapai 36% penggunaan CPU, memory 96% dan kinerja komputer server menurun atau menjadi lemot.



Gambar 5. Tahap Incident

3.4 Respon

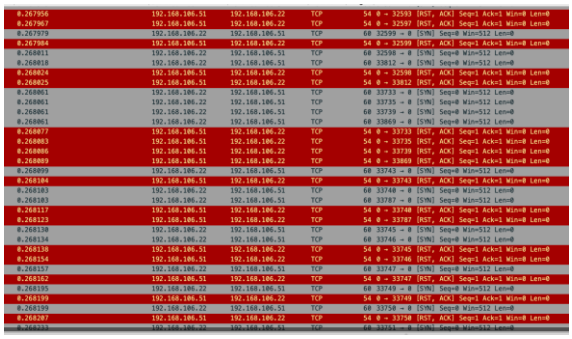
Peneliti melakukan identifikasi secara paralel dengan membatasi akses ke endpoint yang terinfeksi atau sistem yang terdeteksi terkena serangan. Setelah diketahui adanya serangan, peneliti melakukan isolasi pada sistem tersebut. Langkah selanjutnya yang diambil setelah terjadi serangan adalah mengaktifkan firewall pada komputer windows server.



Gambar 6. Tahap Respon

3.5 Collection

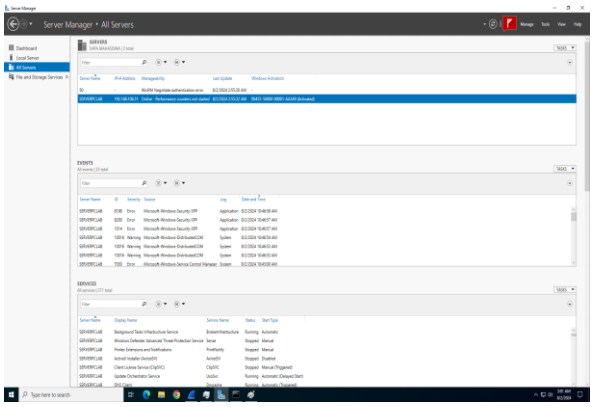
Peneliti melakukan pengambilan log monitoring jaringan menggunakan Wireshark untuk menganalisis trafik anomaly tersebut. Pada tahap ini, dihasilkan penelusuran jejak log lintas jaringan menggunakan Wireshark.



Gambar 7. Tahap Collection

3.6 Preservation

Pada tahapan ini terdapat beberapa data penting berupa bukti digital pada pc server seperti data aplikasi yang mendukung fungsi pembelajaran mahasiswa. Berikut beberapa jenis data dan aplikasi yang ada di PC1 server: Data mahasiswa seperti data pribadi, nama tanggal lahir, nama orang tua, nomor hp, alamat rumah.



Gambar 8. Tahap Preservation

3.7 Examination

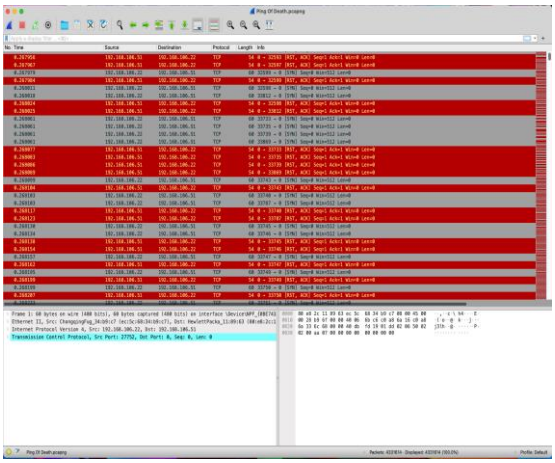
Pada tahap ini, peneliti mendapatkan data dari hasil monitoring log jaringan. Data tersebut diambil dari pengumpulan data menggunakan Wireshark, yang disimpan dalam file dengan ekstensi.pcap.

Ping Of Death.pcapng

Gambar 9. Tahap Examination

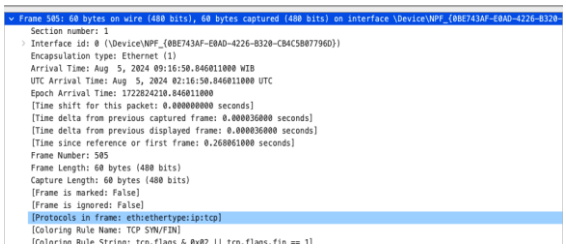
3.8 Investigation

Langkah pertama yang dilakukan setelah terjadi serangan adalah pengolahan data dari file hasil uji coba Ping of Death.pcapng yang diperoleh saat pengumpulan data. Data yang dicari adalah data dengan protokol TCP (Transmission Control Protocol), yang ditandai dengan warna biru pada Wireshark, seperti yang ditunjukkan pada Gambar 4.7. TCP Flood merupakan indikator serangan dari sumber dan jenis serangan DDoS.



Gambar 10. Tahap Investigation

Pada Gambar diatas diketahui alamat IP penyerang adalah 192.168.106.22 Selain itu, terdapat informasi mengenai zona waktu kapan terjadinya serangan tersebut yang ditampilkan pada panel detail paket yang ditandai dengan warna biru.



Gambar 11. Bukti Serangan

Dari hasil panel detail paket, diketahui bahwa serangan terjadi pada tanggal 5 Agustus 2024, pukul 09:16 WIB.

4.9 Presentation

Dalam presentasi ini, peneliti menjelaskan bahwa serangan dilakukan dengan menggunakan jenis serangan Ddos. Serangan dilakukan terhadap komputer windows server dan ditemukan ip penyerang 192.168.106.22, yang mengakibatkan banyaknya permintaan yang dikirim dan diterima oleh komputer windows server. Dampak dari serangan ini adalah peningkatan penggunaan CPU dan memory pada server serta penurunan kinerja komputer windows server, tidak hanya itu dampak berkelanjutan akibat serangan tersebut tidak adanya ketersediaan layanan pada data base yang ada diserver. Analisa lalu lintas jaringan dapat dilihat menggunakan aplikasi Wireshark, dan bukti digital berupa file pcap diperoleh melalui metode forensik digital. Bukti digital dari serangan ini juga diperoleh melalui metode forensik jaringan dengan menggunakan aplikasi Wireshark.

4. KESIMPULAN DAN SARAN

Dalam kesimpulan implementasi pengujian perancangan forensik jaringan ini dapat ditarik kesimpulan sebagai berikut:

1. Melalui tahapan metode forensik jaringan ini peneliti dapat memonitoring ip yang masuk dan ditemukan nomor ip penyerang 192.168.106.22 dengan menggunakan aplikasi wireshark.
2. Melalui tahapan metode forensik jaringan ini peneliti mendapatkan sumber jenis serangan jaringan Denial of service dan bukti serangan dibuktikan dengan

kenaikan trafik yang terlalu tinggi terlihat bahwa setiap 1 detik terjadi 3 paket yang terkirim dan diterima dalam rentang waktu 1 menit sekitar 180 kali paket terkirim dan diterima.

Berdasarkan penelitian yang sudah dilakukan, terdapat saran yang diterapkan oleh penelitian selanjutnya, Diantaranya perlu menggunakan metode selain forensik seperti NIST, OSKAR. Dan juga jenis serangan selain Ddos yaitu Cachr poisoning, DNS Aplication.

DAFTAR PUSTAKA

[1] H. A. Tambunan and Allwine, "Keamanan Jaringan (Firewall) dari Penyerangan Melalui Metode DoS (Denial of Service) Dengan Menggunakan Visual Basic 6.0," *J. Bisantara Inform.*, vol. 1, no. 2, 2019.

[2] I. Ramadhan, "Monitoring Keamanan Jaringan Dengan Snort Ids Menggunakan Metode Forensic Jaringan (Studi Kasus: Cv.Triem Gunung Mas Sejahtera)," *J. Ilm. MIKA AMIK Al Muslim*, vol. 3, no. 1, pp. 13–18, 2019.

[3] B. Fachri and F. H. Harahap, "Simulasi Penggunaan Intrusion Detection System (IDS) Sebagai Keamanan Jaringan dan Komputer," *J. Media Inform. Budidarma*, vol. 4, no. 2, p. 413, 2020.

[4] I. W. Ardiyasa, "Aplikasi Analisis Network Forensic untuk Analisis Serangan pada Syslog Server," *Res. Comput. Inf. Syst. Technol. Manag.*, vol. 2, no. 2, p. 59, 2019.

[5] F. Firmansyah, A. Fadlil, and R. Umar, "Analisis Forensik Metarouter pada Lalu Lintas Jaringan Klien," *Edu Komputika J.*, vol. 6, no. 2, pp. 54–59, 2019.

[6] "(NETWORK SECURITY) Apa itu keamanan komputer dan keamanan jaringan ????"

[7] T. Tasmi, F. Antony, and U. Ubaidillah, "Network Forensik Untuk Menganalisa Trafik Data Game Online," *Klik - J. Ilmu Komput.*, vol. 3, no. 1, pp. 50–58, 2022.

[8] W. W. Septian Geges, "Pengembangan Pencegahan Serangan Distributed Denial of Service (Ddos) Pada Sumber Daya Jaringan Dengan Integrasi Network Behavior Analysis Dan Client Puzzle," *J. Ilm. Teknol. Inf.*, vol. 13, no. 1, pp. 53–67, 2019.

[9] R. T. Novita, I. Gunawan, I. Marleni, O. G. Grasia, and M. N. Valentika, "Analisis Keamanan Wifi Menggunakan Wireshark," *JES (J. Elektro Smart)*, vol. 1, no. 1, pp. 1–3, 2021.

[10] A. Abdul Wahid, "Analisis Metode Waterfall Untuk Pengembangan Sistem Informasi," *J. Ilmu-ilmu Inform. dan Manaj. STMIK*, no. November, pp. 1–5, 2020.

[11] Firda, S. Putri, Y. B. Utomo, and H. Kurniadi, "Analisa Celah Keamanan Pada Website Pemerintah Kabupaten Kediri Menggunakan Metode Penetration Testing Melalui Kali Linux," *Pros. SEMNAS INOTEK (Seminar Nas. Inov. Teknol.*, vol. 7, no. 1, pp. 52–59, 2023.